BOLETÍN DE LA FACULTAD DE DERECHO, núm. 26, 2005

COMERCIO ELECTRÓNICO: TRANSACCIONES SEGURAS Y CONFIDENCIALES. A PROPÓSITO DE UN LIBRO DE RIDOLFI

RIDOLFI, Pierluigi: *Firma digitale e sicurezza informatica. Tecnologie e normative.* 1998, Milano: Franco Angeli, 122 pp.

LUIS EUGENIO OLIVER

Sumario: 1. EL AUTOR Y ESTA OBRA.–2. CRIPTOGRAFÍA Y CODIFICACIÓN.–3. UN SISTEMA DE CODIFICACIÓN ASIMÉTRICA: RSA.–4. CONTROL Y GESTIÓN DE LOS SISTEMAS DE CODIFICACIÓN: [EL MENSAJE VIAJA DE INCÓGNITO].–4.1. Generación de claves: El ente EC generador de claves para la creación de firma.–4.2. Autoridad de certificación: La autoridad AC que produce certificaciones.–5. CONTROL Y GESTIÓN DE LA «IMPRONTA» DEL DOCUMENTO: [EL MENSAJE LLEGA A SU DESTINO INTACTO].–6. FIRMA DIGITAL Y CERTIFICACIÓN.–7. NOTARIOS EN RED: NOTARTEL, DEL CONSEJO NACIONAL DE NOTARIOS.–8. SEGURIDAD Y CONFIDENCIALIDAD DE LOS DATOS DE CARÁCTER PERSONAL.–9. CONSIDERACIONES FINALES.

1. EL AUTOR Y ESTA OBRA

El autor es ingeniero y además docente de la Universidad de Bolonia; fue director central para la Investigación y las innovaciones de la IBM en Italia.

La criptografía, nos dice Ridolfi en el Prefacio de este libro, se está convirtiendo en tema de gran actualidad. ¿Cómo garantizar la privacidad de un documento originado y difundido por vía infor-

mática, asegurar la integridad y certificar la proveniencia? Los problemas, en palabras del mismo Ridolfi, son al mismo tiempo técnicos y legales y reclaman nuevas competencias de tipo transversal, una mezcla de informática, de matemáticas y de derecho.

Abrir en el lector nuevos horizontes técnicos y culturales, ayudarle a determinar, en su campo, el ángulo justo dentro del cuál se puede ocultar la innovación, la eficacia, la eficiencia, el pequeño o gran paso sobre el camino del progreso. Esa es una de las aspiraciones del libro, nos confiesa su autor.

De dos Partes y de dos Apéndices consta la obra «Firma digital...». La Parte primera se dedica a Conceptos generales y aplicaciones. En ella nos llaman la atención, sobre los otros, estos tres capítulos: 2. Criptografía; 5, El comercio electrónico, donde se aborda la cuestión de la seguridad de las transacciones comerciales; y 6, El documento informático, donde se desarrolla el tema de la firma digital y la certificación.

2. CRIPTOGRAFÍA Y CODIFICACIÓN

La criptografía (»escritura escondida») tiene por finalidad hacer posible la transmisión de un mensaje desde un emisor a uno o más destinatarios, de tal modo que éstos, y ningún otro, puedan comprender el significado. En esta sintética definición, se nos explica, intervienen los tres conceptos fundamentales de la criptografía: el *mensaje*, los *interlocutores* (emisor y destinatarios) y el *sistema* de codificación y decodificación.

Sistemas de codificación, advierte Ridolfi, existen muchísimos. Todos se basan en dos pilares: el «método» de codificación y el tipo de «clave». Los métodos se dividen en dos grandes categorías según que se emplee una sola clave o dos. En el método de las dos claves, el emisor codifica el mensaje con la clave pública del destinatario, fácilmente consultable en un elenco; para decodificar el mensaje se precisa la clave privada del destinatario, que sólo él conoce. Lo que se garantiza con el sistema de criptografía es no sólo la privacidad del mensaje, sino también la *integridad* [de su contenido] y la *autenticidad* [de su procedencia].

Al referirse a «Algunos sistemas de criptografía», nuestro autor explica el método de la traslación [de posiciones de caracteres], el método de la correspondencia directa, los métodos binarios o escritura en octetos con componentes de los dígitos binarios (el 0 y el 1).

Los llamados *sistemas de codificación simétrica* se basan en dos procedimientos diversos de codificación y decodificación (uno inverso del otro), pero sobre una sola clave.

Los llamados *sistemas de codificación asimétrica* se basan en la existencia de dos claves y un único procedimiento de codificación y decodificación. Se llaman sistemas de clave pública. Pero, en verdad, el nombre de asimétrico deriva de este hecho: la persona que codifica un mensaje (con la clave pública del destinatario) no está en condiciones de decodificarlo (porque para ello se precisa la clave privada del mismo destinatario).

3. UN SISTEMA DE CODIFICACIÓN ASIMÉTRICA: RSA

Un sistema de codificación asimétrica muy generalizado es el llamado RSA (denominación que se corresponde con las letras iniciales de los respectivos nombres de quienes lo inventaron, en el año 1977: **R**ivert, **S**hamir y **A**dleman, del Massachusetts Institute of Technology). El fundamento matemático del sistema de codificación llamado RSA se halla en un teorema que, en su forma más simple, como textualmente se dice en el libro que estamos comentando, afirma que: si un número entero «a» lo elevamos a la potencia «n» y el resultado es luego dividido por «n», el resto de la división, si «n» es primo, es igual al número de partida, esto es, es igual a «a».

Es lo que ocurre en el siguiente ejemplo: a = 5 y n = 3; 5 elevado a 3 = 125; 125 dividido entre 3 da 40 con un resto de 5, como se trataba de demostrar.

El teorema en cuestión se debe a un matemático francés del XVII, que fue quien lo inventó (Pierre de Fermat, nacido en el 1601, a quien Pascal llamó «el primer hombre del mundo») y a un matemático suizo del XVIII, que fue quien lo divulgó (Leonhard Euler). El llamado «indicador de Euler» de un número natural «n», que se expresa con el símbolo E(n), es el producto de sus factores disminuido cada uno en 1. Siendo «n» el producto de dos números primos «p» y «q», resulta así:

$E(p \cdot q) = (p - 1) \cdot (q - 1)$. Pero si «n» fuese número primo, resultaría así: $E(n) = n - 1$.

El autor de «Firma digital e sicureza informatica» pasa a darnos cuenta, bien que con sólo valor propedéutico, de las distintas fases en que consiste el sistema de codificación asimétrica RSA, contem-

plando estos dos supuestos: [A], si el número «n» fuese número primo y [B] si el número «n» fuese el producto de dos factores números primos.

Respecto al primer supuesto, tratándose de un número primo, el sistema comprende, entre otras, las fases siguientes:

a) Se calcula el indicador de Euler del número «n»;
b) A cada miembro del grupo de usuarios se le asigna una clave «h» (pública), elegida al azar; y se calcula la correspondiente clave «j» (privada) con una fórmula matemática que está en función de «h» y de «E»;
c) Se descompone el texto a transmitir en una serie de trozos de mensaje «m»;
d) Se procede a *codificar* cada uno de los trozos del mensaje m [del mensaje fuente, en claro] obteniendo así el mensaje «mc». El procedimiento consiste en elevar «m» a la potencia «h» (clave pública), dividir luego el resultado por «n» y determinar el resto de esta división: el valor de este resto constituye el mensaje cifrado «mc»;
e) El procedimiento de *decodificar* consiste en elevar «mc» a la potencia «j» (clave privada), dividir luego el resultado por «n» y determinar el resto de esta división: el valor de este resto coincide exactamente con el mensaje original «m»;
f) El procedimiento se repite para todos los trozos del mensaje, para todos los demás «m».

Nuestro autor nos advierte enseguida de la vulnerabilidad de este sistema de codificación y decodificación de un mensaje que toma como punto de partida un número primo: cualquiera está en condiciones de calcular «j» (la clave privada), que se obtiene en función de «h» (la clave pública) y de E (el indicador de Euler).

Pero las cosas cambian radicalmente si «n», en lugar de ser número primo, es el producto de dos números primos «p» y «q». Porque entonces el procedimiento a seguir será el siguiente:

a) Una autoridad central, una Entidad Central, que llamaremos EC, fija un número primo cualquiera «h» universalmente conocido.
b) Para cada miembro del grupo de usuarios EC escoge dos números primos «p» y «q», distintos entre sí y también distintos de «h». Sobre esta base calcula: $n = p \cdot q$; $E = (p - 1) \cdot (q - 1)$; «j», en función de «h» y de «E». Ningún extraño se halla en

condiciones de calcular el valor de «j», porque el algoritmo requiere el conocimiento previo del indicador de Euler de un número que resulta de multiplicar dos números primos.

4. CONTROL Y GESTIÓN DE LOS SISTEMAS DE CODIFICACIÓN: [EL MENSAJE VIAJA DE INCÓGNITO]

4.1. GENERACIÓN DE CLAVES: EL ENTE EC GENERADOR DE CLAVES PARA LA CREACIÓN DE FIRMA

Sea cual sea el sistema de codificación que se use, es preciso que haya alguien que genere las claves, las asigne y haga públicas las que sean públicas. Se necesita, en fin, *un organismo de control* (un Ente Central para la asignación de claves: EC) que lleve a cabo tareas como éstas:

a) establecer los algoritmos de cálculo para la creación de claves y preparar el paquete de programas informáticos para su gestión;

b) recibir las peticiones de asignación de la pareja de claves por parte de los particulares usuarios;

c) elegir una pareja de números primos «p» y «q» todavía no asignados;

d) registrar esta pareja de números en el correspondiente banco de datos (pero sin indicación de la persona a la que han sido asignados);

e) calcular la clave privada «j» y la pública «h»; difundir la pública, por Internet sería un buen modo; comunicar en forma reservada al usuario su clave privada.

Como es lógico, disponer de una clave de codificación y decodificación no es bastante para intercambiar mensajes con plena garantía de autenticidad para quien los reciba. Es preciso involucrar en nuestro juego de claves a un tercero de confianza, a lo que se llama *un ente de certificación,* una autoridad certificadora.

4.2. AUTORIDAD DE CERTIFICACIÓN: LA AUTORIDAD AC QUE PRODUCE CERTIFICACIONES

En opinión de Ridolfi, el modo de operar de una Autoridad de Certificación será:

Primero. AC pide al solicitante de certificación su nombre comercial **F**, su lema de identificación como empresa, su «firma», por decirlo así.

Segundo. AC combina tal lema de identificación con la clave pública *h* de tal solicitante (obtenida de EC).

Tercero. AC codifica el nombre comercial **F** con la clave privada de la propia AC obteniendo la llamada «firma digital» **FD.**

Cuarto. AC envía al solicitante la **FD** (que el solicitante deberá adjuntar a todos los mensajes de salida).

Quinto. AC provee al solicitante de un ***paquete de software***, a instalar en su PC, activable con apropiados procedimientos de seguridad, en condiciones de cumplir las siguientes funciones en las sucesivas fases de implantación, de envío y de lectura. [1] En la fase de **implantación** del procedimiento: *memorizar la clave privada* del solicitante en una zona protegida del PC de modo que no pueda ser leída ni alterada por ninguno. [2] En la fase de **envío** de mensajes: *codificar los mensajes con la clave privada* y firmarlos automáticamente ya sea con la propia **F** ya sea con la propia **FD.** [3] En fase de **lectura** de mensajes: (a) decodificar con la clave pública de la Autoridad de Certificación (introducida en el programa) la **FD** recibida y obtener así la firma [codificada] del remitente a comparar con la recibida en claro; (b) conectarse (por ejemplo, vía Internet) a AC y obtener la clave pública del remitente; (c) decodificar mediante la clave pública obtenida el mensaje recibido.

El texto se ilustra con oportunos y muy claros ejemplos. Una de las conclusiones más llamativas de estos mecanismos de codificación y decodificación es que *lo codificado con una clave privada se decodifica con la correspondiente clave pública*.

Por otra parte, en toda esta trama de sujetos e instrumentos componentes del sistema de creación y verificación de firmas y del sistema de certificaciones de firmas, cabe que destaquemos estos siete componentes: ***Uno:*** Registro de prestadores de servicios. ***Dos:*** Prestadores de servicios de firma y/o de certificaciones. ***Tres:*** *programas generadores de* ***productos de firma:*** *de creación o de verificación de firma* [son ***programas*** para producción de dispositivos de creación de firma]. ***Cuatro:*** *programas generadores de* ***firma,*** *dispositivos de creación de firma: aplican los datos de creación de firma, esto es, la claves de codificación* [son ***programas*** generadores de información que vale como firma]. ***Cinco:*** datos de creación de firma: ***claves*** de codificación. ***Seis:*** ENTE CENTRAL PARA LA ASIGNACION DE CLA-

VES. ***Siete:*** AUTORIDAD DE CERTIFICACION, también llamados «terceros de confianza». Su función primordial, como más adelante se explicará con más detalle, consiste en garantizar la *correspondencia entre clave pública y el sujeto titular de la misma.*

En resumen, un sistema de firma digital requiere: a) el elemento material de los programas y las claves de codificación y b) el elemento personal de los firmantes y la entidad certificadora de firmas —para la designación de esta entidad proponemos el nombre de CERTIFICANTE o aún el de GARANTE de correspondencia entre la clave pública del firmante y su firma—.

5. CONTROL Y GESTIÓN DE LA «IMPRONTA» DEL DOCUMENTO: [EL MENSAJE LLEGA A SU DESTINO INTACTO]

No basta que el mensaje que el emisor envía al receptor viaje de incógnito; es preciso que además llegue a su destino sin cambios, sin manipulaciones, intacto: aún sin haber sido observado por ninguno. ¿Cómo conseguirlo? Por medio de la impronta.

Qué es la impronta. Nos dice bien Ridolfi que «dado un documento constituido por un texto, se le subdivide en una secuencia de tramos consecutivos de longitud fija, llamados *segmentos.* Con el término «impronta» [huella] se entiende un nuevo segmento obtenido del texto originario mediante un determinado procedimiento de cálculo». [Eso es en el fondo cualquier programa informático compuesto de algoritmos: un procedimiento de cálculo].

Textos idénticos producen improntas idénticas; que existan textos diversos que produzcan la misma impronta, eventualidad poco probable: contando con que la extensión de los segmentos sea de 64 bits (esto es, de 64 dígitos binarios), la probabilidad es de uno sobre dieciséis millones de millones (2 elevado a 64), número superior al total de todos los documentos producidos en la historia de toda la humanidad, advierte nuestro autor (*Ibid.*)

Para el cálculo de la impronta las operaciones comienzan por multiplicar el primer segmento del texto por el segundo; se sigue dividiendo el resultado en dos segmentos; después se suman las dos mitades; el resultado obtenido se multiplica por el tercer segmento, etc. etc. Se llegan a obtener dos improntas, G y H: la una partiendo del primer segmento y la otra partiendo del último segmento en que quedó dividido el texto. La impronta final resulta de la suma de G y

de H. Este método, que parece muy complejo, se presta fácilmente a una elaboración automática.

La impronta consta de menos bits que el texto originario; y, por tanto, no es posible construir tal texto partiendo de la impronta: pero ciertamente que textos idénticos producen idénticas improntas. La impronta, concluye nuestro autor, asume el valor de garantía de identidad del documento [p. 91]. Añadamos por nuestra parte que en muchos textos escritos en español hemos leído el término «resumen» del texto original para referirse a lo que en el libro, en italiano, de Ridolfi se llama «impronta». Verdaderamente llamar a la impronta un resumen nos parece que induce a confusión: hablemos, por tanto, de impronta o huella obtenida por procedimientos de cálculo efectuados sobre el texto original como garantía de identidad del documento.

6. FIRMA DIGITAL Y CERTIFICACIÓN

Como advierte nuestro autor, la llamada Ley Bassanini, de 15 de marzo de 1997, sobre simplificación administrativa del Estado, reconoció valor legal a los documentos informáticos [p. 60]. Porque, como a renglón seguido se argumenta, la eliminación del papel es un prerrequisito para el incremento de productividad de cualquier sistema administrativo empresarial y consecuentemente también del estatal.

Con el Reglamento para la aplicación de la citada ley (DPR de 10 de noviembre de 1999 sobre el documento informático y la firma digital) se da un paso definitivo en el ámbito de la validez legal de la documentación digital. Este reglamento, en frase de Ridolfi, permite incluso utilizar las técnicas de criptografía para garantizar la corrección del documento archivado y certificar la conformidad del original en soporte papel, que ya no tiene razón de ser, y puede ser destruido, desde el momento en que exista una copia informática del mismo. Se trata, se concluye, de «una norma verdaderamente revolucionaria que, cuando de verdad venga aplicada, hará desparecer los archivos en soporte papel», *gli archivi cartacei.*

Vale la pena reproducir aquí la definición que da de «firma digital» el DPR/513 de 10 de noviembre de 1997 sobre documento informático y firma digital. Es el siguiente:

> Firma digital es *el* ***resultado del procedimiento*** *informático (validación) basado sobre un sistema de claves asimétricas en pareja, una*

pública y otra privada, que permite al suscriptor a través de la clave privada y al destinatario a través de la clave pública, respectivamente, poner de manifiesto y verificar la ***procedencia y la integridad de un documento informático*** *o de un conjunto de documentos informáticos.*

La validación, ¿qué es? Según nuestro autor, que reelabora la definición que el citado DPR ofrece, la validación consiste en [el acto de] *generar* y poner a disposición de la firma digital o de *verificar* su validez [las cursivas son nuestras]. Un caso particular de validación, añade, es la validación temporal, con la que viene atribuida a un documento una fecha y un horario ciertos.

La certificación, ¿para qué sirve? La certificación garantiza la *correspondencia entre clave pública y el sujeto titular de la misma*, que viene identificado en claro. La validación y la certificación requieren ambas, como puede suponerse, complejos procedimientos informáticos. Así lo dice Ridolfi.

Dos son las entidades a quienes compete gestionar lo relacionado con las claves asimétricas: el Ente Central de asignación de claves (EC) y la Autoridad de Certificación (AC), bien que este nombre de «autoridad», consagrado por el uso, provenga de Estados Unidos, donde hay una correcta adecuación entre el término y su significado, y no tenga sentido usarlo en Italia (ni tampoco en España), donde no está previsto que el «certificador» sea una «autoridad».

Nada se dice en el DPR citado, sobre documento electrónico y firma digital, referente a un Entre Central de certificación. Esta norma se limita a decir que «cualquiera que pretenda utilizar un sistema de claves asimétricas de cifrado debe proveerse de una idónea pareja de claves y *hacer pública una de ellas mediante el procedimiento de certificación*» [las cursivas son nuestras]. Incluso el reglamento no excluye que sea el mismo usuario quien se encargue de generar, con el programa idóneo, el par de llaves que necesite.

7. NOTARIOS EN RED: NOTARTEL, DEL CONSEJO NACIONAL DE NOTARIOS

En Italia el Consejo Nacional de Notarios ha dado vida a Notartel. Para comprar un inmueble ya no será necesario, nos dice Ridolfi, que adquirente y vendedor, o sus representantes, se encuentren ante el mismo notario: será posible hacerlo en presencia de notarios diversos, lejos uno de otro. La compraventa, en efecto, vendrá certificada por una escritura privada autenticada, obtenida en modo telemático. [Y pasa a describir cómo tal cosa se conseguirá]:

El vendedor, ante uno de los dos notarios suscribirá el acto de venta con la propia firma digital, que el notario se prestará a autenticar a su vez utilizando su propia firma digital. El contrato será enviado electrónicamente a través de la red Notartel al despacho del otro notario, donde se encuentra el comprador, que realizará una operación análoga. En el futuro, concluye nuestro autor, también las variaciones catastrales podrán ser llevadas a cabo por el notario directamente en forma telemática (p. 65).

Después se cantan las excelencias que para el mundo de magistrados, abogados y fuerzas del orden público traerán el documento informático y la firma digital. Por ejemplo: una sentencia podrá ser escrita directamente sobre el computador y no ser ya escrita ni firmada de la manera convencional, pero manteniendo plenamente su valor; los abogados podrán hacer llegar sus propias actuaciones por vía telemática, sin moverse de su despacho.

Para imaginar el tipo de futuro que nos aguarda, sin papel y con una burocracia más veloz y eficiente que la actual, nuestro autor señala en breves pinceladas y citando una fecha por lustro lo que significaron el fax y la tarjeta de crédito en el 1975, el ordenador personal en el 1980, los teléfonos móviles en el 1985 y la difusión del uso de Internet en el 1990. No es ninguna utopía, se nos viene a decir, imaginar lo que ocurrirá dentro de cinco años cuando se difunda el uso del documento electrónico y la firma digital. Definitivamente la sociedad va a cambiar de hábitos, añadamos, y los operadores del derecho van a cambiar de modos de proceder en su profesión.

8. SEGURIDAD Y CONFIDENCIALIDAD DE LOS DATOS DE CARÁCTER PERSONAL

Como a nadie se oculta, el tratamiento automatizado de la información, que en numerosas ocasiones lleva implícito el tratamiento automatizado de la información alusiva a la identidad y circunstancias de determinadas personas, conlleva el peligro de que, sin su consentimiento se difundan sus datos privados, si no se toman las oportunas medidas de protección de su privacidad.

A conjurar dicho peligro vienen las leyes de protección legal de datos personales que están vigentes hoy en la generalidad de los países. A este respecto nuestro autor trae a colación la Ley italiana 675/96 sobre la Protección de Datos Personales que tiene como fin

«garantizar que el tratamiento de los datos personales se desarrolle en el respeto a los derechos, de las libertades fundamentales y de la dignidad de las personas físicas».

También para los datos contenidos en las direcciones personales es preciso observar las normas de protección y seguridad de los mismos. La disciplina de la seguridad informática es algo muy amplio y está en constantes y rápidas transformaciones (pp. 71 a 73). No es el libro de Ridolfi el lugar indicado para un análisis pormenorizado de la Ley a la que, con motivo de la protección y seguridad de los datos personales, se alude. Pero sí era necesaria, como así se ha hecho, una alusión al tema.

9. CONSIDERACIONES FINALES

Estimamos que el libro de Ridolfi es un libro necesario: 1, porque es un buen *modo de iniciación* al estudio del comercio electrónico; 2, porque, de un modo relativamente asequible, *sienta las bases técnicas* del intercambio telemático de mensajes con garantías de autenticidad, integridad y confidencialidad; 3, porque el planteamiento de sus contenidos es realmente bifronte, complementándose recíprocamente estos dos enfoques.

«Firma digítale e sicureza informática» es un libro breve, de poco más de cien páginas, bien estructurado en 9 capítulos: los siete primeros de la Parte primera, y de la Parte segunda los dos últimos.

En la Primera parte, referida a Conceptos generales y aplicaciones, hay un capítulo, el 2, dedicado a la Criptografía, en el que se aborda la Invulnerabilidad del sistema criptográfico RSA. Y otro, el 7, dedicado a La Protección de Datos Personales. Los restantes se titulan Firma digital y organización (el cap. 1); Autenticidad, integridad y certificación (el 3); El correo electrónico (el 4); El comercio electrónico (el 5) y El documento informático (el 6).

En la Parte segunda, Métodos matemáticos y sistemáticos, se trata de Elementos de aritmética modular (cap. 8) y de Profundizaciones técnicas (cap. 9).

Se completa el contenido del libro con dos apéndices que curiosamente siguen la línea del planteamiento bipolar, técnicoinformático y legislativo, del conjunto: Apéndice I, Programas (entiéndase programas informáticos). Apéndice II, El DPR 10 noviembre 1997, n. 513 sobre documento informático y firma digital, un texto de con-

siderable interés que se presta a un análisis comparativo respecto a la actual directiva europea sobre el mismo asunto.

Las dos últimas páginas del libro se dedican a Bibliografía esencial. Aquí se recoge la referencia a dos obras de carácter técnico, editadas en inglés: «Crittologia» y «Primes and Programming». Además se inserta una tabla de sitios web relacionados con el tema, entre los que figura uno que incluye informaciones actualizadas sobre los contenidos del libro objeto de nuestros comentarios. La dirección de tal sitio es la siguiente: *www.erresoft.com/firmadigitale*.